para Mac OS X Server

Manual de administrador

Doctor Web

A Doctor Web desenvolve e distribui soluções Dr.Web® para a segurança de informações, que fornecem proteção eficiente contra softwares mal-intencionados e lixo eletrônico.

Os clientes Doctor Web são usuários domésticos, empresas governamentais, pequenas empresas e grandes corporações de todo o mundo.

A soluções de antivírus Dr.Web são conhecidas desde 1992 pela contínua excelência na detecção de malware e pela conformidade com os padrões internacionais de segurança de informações. Os certificados e prêmios recebidos pelas soluções Dr.Web, assim como o amplo uso de nossos produtos em todo o mundo, são a melhor prova da confiança excepcional nos produtos da empresa.

Agradecemos a todos os nossos clientes pelo apoio e pela confiança nos produtos Dr.Web!

Conteúdo

Convenções do documento

Os seguintes símbolos e convenções são usados neste manual:

Convenção	Descrição
Negrito	Nomes de botões e outros elementos da interface gráfica do usuário (GUI), e dados que devem ser inseridos pelo usuário, exatamente como mostrados no guia.
Verde e em negrito	Nomes de produtos e componentes da **Dr.Web**.
Verde e sublinhado	Hiperlinks de tópicos e páginas da Web.
Itálico	Espaços reservados que representam informações que devem ser fornecidas pelo usuário. Em entradas de linha de comando, indica valores de parâmetros. Além disso, pode indicar um termo com a função de definição.
LETRAS EM CAIXA ALTA	Nomes de teclas e sequências de teclas.
Sinal de menos ("-")	Indica uma combinação de teclas. Por exemplo, COMMAND-Q significa segurar a tecla COMMAND e pressionar a tecla Q.
Ponto de exclamação	Um aviso sobre possíveis erros ou comentários importantes.

As seguintes abreviações são usadas neste manual:

- CPU: unidade de processamento central
- GUI: interface gráfica do usuário
- SO: sistema operacional
- RAM: memória de acesso aleatório

Capítulo 1. Introdução

Obrigado por adquirir o **Antivírus Dr.Web para Mac OS X** (doravante denominado **Dr.Web Anti-virus**). Este produto oferece proteção confiável contra vários tipos de ameaças, com o uso das mais avançadas tecnologias de detecção e neutralização de vírus.

Este manual tem como objetivo ajudar os administradores de servidores que utilizam Mac OS X Server, na instalação e no uso do **Dr.Web Anti-virus**.

Sobre o Dr.Web Anti-virus

Dr.Web Anti-virus é uma solução de antivírus que ajuda os administradores de servidores que utilizam Mac OS X Server a protegerem seus sistemas contra vírus e outros tipos de ameaças.

Os componentes de base do programa (*mecanismo de antivírus* e *bancos de dados de vírus*), além de serem extremamente eficazes e econômicos, também podem ser usados em diferentes plataformas, permitindo que os especialistas da **Doctor Web** criem soluções de antivírus completas, para diferentes sistemas operacionais. Os componentes do **Dr.Web Anti-virus** são constantemente atualizados, e os bancos de dados de vírus são sempre suplementados com novas assinaturas, para garantir uma proteção atualizada. Além disso, um analisador heurístico é utilizado para fornecer proteção adicional contra vírus desconhecidos.

Componentes e funções principais

O **Dr.Web Anti-virus** consiste nos seguintes componentes, que executam suas funções específicas:

Componente	Descrição
SpIDer Guard	É um componente de antivírus residente que verifica todos os arquivos (que estão em uso) em tempo real.
SpIDer Gate	Este componente verifica o tráfego HTTP recebido e bloqueia todos os objetos mal-intencionados. Também é usado para controlar o acesso a recursos da Web.
Verificador	Este componente de detecção de vírus é usado para: • Verificação expressa, completa e personalizada do sistema, sob demanda do usuário.. • Neutralização de ameaças detectadas (curar, excluir, mover para quarentena). A ação é selecionada pelo usuário de forma manual ou automática, de acordo com as configurações do **Dr.Web Anti-virus** para o tipo de ameaça correspondente.
Quarentena	É um tipo especial de pasta, usada para isolar arquivos infectados e outras ameaças, para que não danifiquem o sistema.
Atualizador	É um utilitário de atualização automatizado, usado para atualizar bancos de dados de vírus e outros componentes do programa.
Gerenciador de Licenças	Este componente simplifica o gerenciamento de arquivos de chave de licença, permite o recebimento de arquivos de chave de licença e demonstração, a exibição de informações sobre esses arquivos e a renovação da sua licença.

As configurações flexíveis do **Dr.Web Anti-virus** permitem a configuração de notificações sonoras e visuais de diversos eventos, ações automáticas aplicadas pelo antivírus para detectar ameaças, periodicidade de atualização, listas de pastas e arquivos excluídos da verificação etc.

Capítulo 2. Instalação e remoção

O **Dr.Web Anti-virus** é distribuído em um único arquivo de imagem de disco (**drweb-1003-mac.dmg**). O arquivo pode ser encontrado no CD/DVD do produto ou baixado pela Internet, no site oficinal da **Doctor Web**, em http://www.drweb.com.

O **Dr.Web Anti-virus** não é compatível com outros softwares de antivírus, incluindo suas versões anteriores. A instalação de dois programas de antivírus no mesmo computador pode causar falhas no sistema e perda de dados importantes. Se você já tiver um software de antivírus instalado, desinstale-o, antes de iniciar a instalação de um novo antivírus.

Requisitos do sistema

O **Dr.Web Anti-virus** pode ser instalado em um computador com Mac OS X Server 10.7 ou posterior. Os demais requisitos são semelhantes aos do sistema operacional.

Instalação e remoção do antivírus

O software **Dr.Web Anti-virus** é distribuído em um único arquivo de imagem de disco (**drweb-1003-mac.dmg**).

Para instalar o Dr.Web Anti-virus

1. Clique duas vezes em **drweb-1003-mac.dmg** para montar a imagem, se for necessário.
2. A janela do Contrato de Licença será aberta. Você deve ler e aceitar o contrato, para continuar a instalação.
3. Arraste o arquivo do aplicativo da imagem de disco até a pasta **Aplicativos**, no seu Mac.

Para desinstalar o Dr.Web Anti-virus

Para excluir o **Dr.Web Anti-virus**, basta mover o aplicativo para a **Lixeira**. Se for necessário, insira o nome de usuário e a senha da conta de administrador, na caixa de diálogo correspondente.

Capítulo 3. Gerenciamento de licenças

Para usar o **Dr.Web Anti-virus** por um período estendido, você precisa ativar uma licença. Você pode adquirir uma licença com o produto ou no site oficial da **Doctor Web**. Com uma licença, você pode aproveitar todos os recursos do produto durante todo o período. Os parâmetros do arquivo de chave são definidos de acordo com o contrato de licença de software. Para registrar uma nova licença, renove-a depois que ela expirar ou obtenha uma nova licença. Um componente especial, o **Gerenciador de Licenças**, é utilizado.

É recomendável registrar a licença após a instalação, porque ela desbloqueia as atualizações, a proteção constante e os recursos de verificação sob demanda.

Se você quiser avaliar o produto antes de comprá-lo, pode ativar um período de demonstração. A versão demo oferece toda funcionalidade dos componentes principais, mas o período de validade é consideravelmente limitado.

Você pode ativar um período de demonstração no mesmo computador uma vez por ano, no máximo.

O período de demonstração tem a duração de:

- 3 meses. Para isso, registre-se no site oficial da **Doctor Web** e receba um número de série.
- 1 mês. Para esse propósito, não é necessário ter um número de série nem dados de registro.

Arquivo de chave de licença

O tipo de licença é determinado por um arquivo especial, chamado *arquivo de chave*. O arquivo de chave contém as seguintes informações:

- A duração da licença do antivírus
- A lista de componentes que um usuário pode usar
- Outras restrições (por exemplo, o número de usuários que podem usar o aplicativo)

Uma chave *válida* para o arquivo do **Dr.Web Anti-virus** deve seguir os seguintes critérios:

- A licença não expirou
- Todos os componentes de antivírus requeridos pelo produto são licenciados
- A integridade do arquivo de chave não foi violada

Se qualquer uma das condições for violada, o arquivo de chave se torna *inválido*, e o **Dr.Web Anti-virus** deixa de detectar e neutralizar programas mal-intencionados nos arquivos, na memória e em emails.

O arquivo de chave apresenta a extensão .key e pode ser recebido durante o procedimento de registro da licença, durante a primeira inicialização do **Dr.Web Anti-virus**, por meio do Gerenciador de Licenças.

Os parâmetros do arquivo de chave que especificam os direitos do usuário são definidos de acordo com o Contrato de Licença. O arquivo também contém informações sobre o usuário e sobre o vendedor do antivírus.

Recomendamos que você mantenha o arquivo de chave até que a licença ou período de demonstração expire.

O arquivo de chave de um período de demonstração só pode ser usado no computador onde o procedimento de registro foi realizado.

Gerenciador de Licenças

Para abrir o **Gerenciador de Licenças**, clique em **Gerenciador de Licenças**, no menu do aplicativo (a barra de menu fica na parte superior da área de trabalho principal), ou clique na seção de informações sobre licenças, na janela principal do aplicativo.

A janela **Gerenciador de Licenças** exibe as informações sobre sua licença atual. O botão **Obter nova licença** permite que você registre sua licença do **Dr.Web Anti-virus** ou renove uma licença que já expirou.

Registro de licença

Após a instalação, você precisa registrar o **Dr.Web Anti-virus**, para confirmar a legitimidade do uso do antivírus e desbloquear os recursos de atualização, proteção constante e verificação sob demanda.

Quando você executa o **Dr.Web Anti-virus** pela primeira vez, o registro é iniciado automaticamente. Você também pode iniciar o registro a partir do Gerenciador de Licenças, clicando em **Obter nova licença**.

Para ativar uma nova licença

1. Se você tiver um número de série para ativação de uma licença ou um período de demonstração de 3 meses, na primeira etapa do procedimento de registro, clique em **Ativar licença**.
2. Insira o número de série e clique em **Avançar**. Se você estiver ativando um período de demonstração, vá para a etapa 5.
3. Caso você tenha uma licença anterior, informe o número de série dela ou o arquivo de chave correspondente. Selecione a opção correspondente, insira o número de série ou arraste o arquivo de chave até a área pontilhada (como alternativa, clique na área para navegar até o arquivo de chave e selecioná-lo).

   Se você já foi usuário do **Dr.Web Anti-virus** anteriormente e está registrando uma nova licença, poderá estender sua nova licença por mais 150 dias. Se você estiver registrando uma renovação de licença e não fornecer um arquivo de chave de licença anterior, seu novo período de licença será reduzido em 150 dias.

   Clique em **Avançar**.
4. Insira seus dados pessoais (nome, sobrenome e email), selecione o país e o nome da cidade. Todos os campos obrigatórios devem ser preenchidos. Caso queira receber novidades da **Doctor Web** por email, marque a caixa de seleção correspondente. Clique em **Avançar**.
5. O arquivo de chave de licença será baixado e instalado no seu Mac. Normalmente, este procedimento não requer sua participação ativa. Clique em **Avançar**. Se o procedimento de ativação for concluído com êxito, você verá a mensagem correspondente, informando o período de validade da licença ou da demonstração. Clique em **Concluir**. Se a ativação falhar, uma mensagem de erro será exibida.

Para obter a versão demo

Se você instalou o **Dr.Web Anti-virus** com o intuito de avaliar o produto, clique em **Obter versão demo.**. Você pode ativar um período de demonstração para avaliar o **Dr.Web Anti-virus**:

- Por 3 meses. Para isso, registre-se no site e receba um número de série.

Depois que você concluir o questionário, o número de série exigido para ativar o período de avaliação de 3 meses será enviado para o endereço de email especificado.

- Por 1 mês. Para esse propósito, não é necessário ter um número de série nem dados de registro. O arquivo de chave de licença correspondente será baixado e instalado automaticamente.

Para comprar uma licença

Se você não tiver um número de série, na primeira etapa do procedimento de registro, clique em **Comprar licença**, para adquirir a licença da loja online da **Doctor Web**.

Recomendamos que você mantenha o arquivo de chave até a data de expiração. Se você reinstalar o produto ou instalá-lo em vários computadores, poderá usar o aquivo de chave de licença registrado anteriormente.

Para instalar o arquivo de chave existente

1. Na primeira etapa do procedimento de registro, clique em **Outros tipos de ativação**.
2. Caso você já tenha um arquivo de chave ou um arquivo de configuração necessário para se conectar a um servidor de proteção central, arraste-o até a área pontilhada ou clique para navegar e selecionar o arquivo.
3. Para registrar sua licença, clique em **Avançar**. Normalmente, este procedimento não requer sua participação ativa.

Registro subsequente

Se você perder o arquivo de chave, poderá precisar reativar uma licença ou um período de demonstração.

Ao reativar uma licença ou um período de demonstração, você recebe o mesmo arquivo de chave que recebeu durante o registro anterior, desde que o período de validade não tenha expirado.

Um período de demonstração só pode ser reativado no computador onde o procedimento de registro foi realizado.

O número de solicitações de recebimento de um arquivo de chave é limitado. Um número de série só pode ser registrado 25 vezes, no máximo. O arquivo de chave não será enviado, se houver mais solicitações. Nesse caso, entre em contato com o suporte técnico, para receber um arquivo de chave que você perdeu, descrevendo o problema em detalhes, incluindo o número de série e os dados pessoais que você informou durante o registro.

Capítulo 4. Funções básicas

Você pode acessar todas as funções principais na janela do **Dr.Web Anti-virus** (veja a imagem abaixo). Esta janela apresenta seções que ajudam você a controlar e acessar os componentes de antivírus:

Seção	Descrição
Mesa de controle	Nesta seção, você pode: • Habilitar ou desabilitar a proteção antivírus constante. • Habilitar ou desabilitar a verificação do tráfego na Web. • Ver informações sobre a última verificação e iniciar uma verificação do sistema expressa ou completa, ou verificar apenas pastas e arquivos críticos. • Ver informações sobre a última atualização dos bancos de dados de vírus e iniciar uma atualização manualmente, se for necessário. • Ver informações sobre a licença atual e executar o Gerenciador de Licenças, se for necessário. • Abrir a seção **Ameaças** ou **Meu Dr.Web**.
Ameaças	Permite que você acesse a lista de ameaças detectadas, selecione ações para aplicar a elas e abra o conteúdo da Quarentena.
Meu Dr.Web	Permite que você veja as novidades e últimas ofertas especiais da **Doctor Web**, leia informações sobre vírus e abra sua página pessoal no site oficial da **Doctor Web**, onde você pode ver informações sobre sua licença, bancos de dados de vírus e a atualização mais recente, renovar a licença, entrar em contato com o suporte técnico etc.

Imagem 1. Janela principal do aplicativo.

Iniciar e fechar o antivírus

Para iniciar o Dr.Web Anti-virus

Selecione uma destas opções:

- No Localizador, abra a pasta **Aplicativos** e clique duas vezes em **Dr.Web para Mac OS X**;
- Inicie o Launchpad e selecione o **Dr.Web para Mac OS X**, para iniciá-lo.

Quando o aplicativo é inicializado, as configurações de atualização são verificadas, e as atualizações são baixadas, se necessário.

Na primeira inicialização do aplicativo, os bancos de dados de vírus são atualizados para a versão mais recente no momento. Isso pode levar algum tempo.

Para fechar o Dr.Web Anti-virus

Selecione uma destas opções:

- Clique no item **Fechar Dr.Web para Mac OS X**, no menu do aplicativo (a barra de menu fica na parte superior da área de trabalho principal).
- Clique e segure o ícone do aplicativo no Dock e, em seguida, selecione **Fechar**, no menu.
- Pressione COMMAND-Q no teclado, quando o **Dr.Web Anti-virus** estiver ativo.

Quando você fecha o **Dr.Web Anti-virus**, o **SpIDer Guard** continua ativo. Ele é um monitor antivírus residente, que verifica em tempo real todos os arquivos que são usados.

Atualizar o antivírus

As soluções de antivírus da **Doctor Web** usam bancos de dados de vírus do **Dr.Web** para detectar softwares mal-intencionados. Esses bancos de dados contêm detalhes e assinaturas de todas as ameaças de vírus conhecidas no momento em que o produto foi lançado. No entanto, as ameaças de vírus modernas se caracterizam pela rápida evolução e modificação. Em questão de dias ou apenas horas, surgem novos vírus e programas mal-intencionados. Para mitigar o risco de infecção durante o período da licença, a **Doctor Web** fornece atualizações regulares nos bancos de dados de vírus e componentes dos produtos, pela Internet. Com as atualizações, o **Dr.Web Anti-virus** recebe informações necessárias para detectar novos vírus, impedir que eles se espalhem e, às vezes, curar arquivos infectados que antes eram incuráveis. De tempos em tempos, as atualizações também incluem melhorias nos algoritmos de antivírus e correções de bugs no software e na documentação.

A atualização dos componentes e dos bancos de dados de vírus do **Dr.Web Anti-virus** garante que sua proteção esteja sempre atualizada e pronta para qualquer tipo novo de ameaça. A atualização é realizada por um componente especial chamado **Atualizador**.

Na primeira inicialização do **Dr.Web Anti-virus**, é preciso atualizar os bancos de dados de vírus para a versão mais recente no momento. Outras atualizações serão realizadas periodicamente, no intervalo especificado nas preferências do **Dr.Web Anti-virus**.

Configurar o intervalo de atualizações

1. No menu do aplicativo, clique em **Preferências** e abra a guia **Principal**.
2. Selecione um intervalo para as atualizações.

Proteção antivírus constante

A proteção antivírus constante é realizada por um componente residente chamado **SpIDer Guard**. O componente verifica em tempo real todos os arquivos acessados pelo usuário ou pelos programas e processos em execução no seu Mac. Por padrão, ele é habilitado assim que você instala e registra o **Dr.Web Anti-virus**. Quando uma ameaça é detectada, o SpIDer Guard exibe um aviso e aplica ações de acordo com as preferências de antivírus preferências.

Para habilitar ou desabilitar o SpIDer Guard

- Na seção **Mesa de controle** da janela principal (veja a Imagem 1), habilite/desabilite a opção **SpIDer Guard**.
- Clique no ícone do **Dr.Web Anti-virus** na barra de menus e selecione o item correspondente.

Somente usuários com privilégios de administrador podem desabilitar o **SpIDer Guard**.

Tenha muito cuidado ao usar esta opção! Enquanto as funções do **SpIDer Guard** estiverem desabilitadas, evite se conectar à Internet e, antes de acessar mídias removíveis, verifique-as com o uso do **Verificador**.

Verificação do sistema sob demanda

Dr.Web Anti-virus verifica sob demanda os objetos no sistema de arquivos e detecta diversas ameaças que possam estar presentes no sistema, ainda que inativas. Para proteger o computador, é necessário executar uma verificação do sistema com o **Dr.Web Anti-virus** periodicamente.

A carga do processo aumenta durante a verificação, o que pode levar a um rápido esgotamento da bateria. Recomendamos iniciar a verificação quando o computador portátil estiver conectado à energia elétrica.

Para iniciar a verificação do sistema

1. Na janela principal do **Dr.Web Anti-virus**, selecione o modo de verificação:
   - **Verificação expressa** – executa uma rápida verificação das partes mais vulneráveis do sistema, apenas.
   - **Verificação completa** – executa uma verificação completa de todo o sistema de arquivos.

   Você pode pressionar as combinações de teclas de atalho CONTROL-COMMAND-E e CONTROL-COMMAND-F no teclado, para iniciar a verificação expressa ou completa.

2. Para verificar somente determinados arquivos e pastas, arraste-os até a janela principal do aplicativo ou clique na área pontilhada, na parte esquerda da janela, para selecionar os objetos.

   Na lista de objetos, selecione arquivos e pastas que você deseja verificar:

   - Para adicionar um objeto à lista, clique em +, na lista de objetos, ou simplesmente arraste o objeto até a lista.
   - Para excluir um objeto da lista, selecione-o e clique em − ou arraste-o para fora da janela do aplicativo.

   Clique em **Iniciar verificação** para começar a verificar os objetos selecionados.

Para verificar um arquivo ou uma pasta, a partir do menu de contexto

Selecione **Verificar com o Dr.Web**, no menu de contexto do arquivo ou no ícone da pasta, na Área de Trabalho ou no Localizador.

Quando você inicia a verificação, a janela principal muda para a seção de resultados (veja a ilustração abaixo). Durante a verificação, esta janela exibe as seguintes informações:

- hora de início da verificação
- número de objetos verificados
- tempo restante para o final da verificação
- número de ameaças detectadas
- nome do arquivo que está sendo verificado no momento

O resumo estatístico da sessão de verificação atual é exibido na parte inferior da janela.

Você pode pausar ou interromper a verificação, usando os botões **Pausar** e **Interromper**.

Imagem 2. Ver os resultados da verificação.

Alguns arquivos podem ser omitidos durante a verificação, porque estão corrompidos ou protegidos por senha. Se houver arquivos compactados na lista de objetos ignorados, tente extraí-los antes da verificação.

O **Dr.Web Anti-virus** pode exigir privilégios de administrador para acessar e verificar áreas críticas do disco rígido. Para conceder privilégios de administrador ao **Dr.Web Anti-virus**:

- Pressione a combinação COMMAND-SHIFT-A no teclado e insira a senha de administrador.
- Clique no ícone de cadeado, na parte inferior da janela, e insira a senha de administrador.

Neutralizar ameaças

Para neutralizar ameaças, você pode especificar as ações automáticas ou aplicar ações às ameaças manualmente. Para ver a lista de ameaças detectadas e aplicar ações para neutralizá-las, abra a guia **Ameaças**, na janela principal do aplicativo (veja a ilustração abaixo).
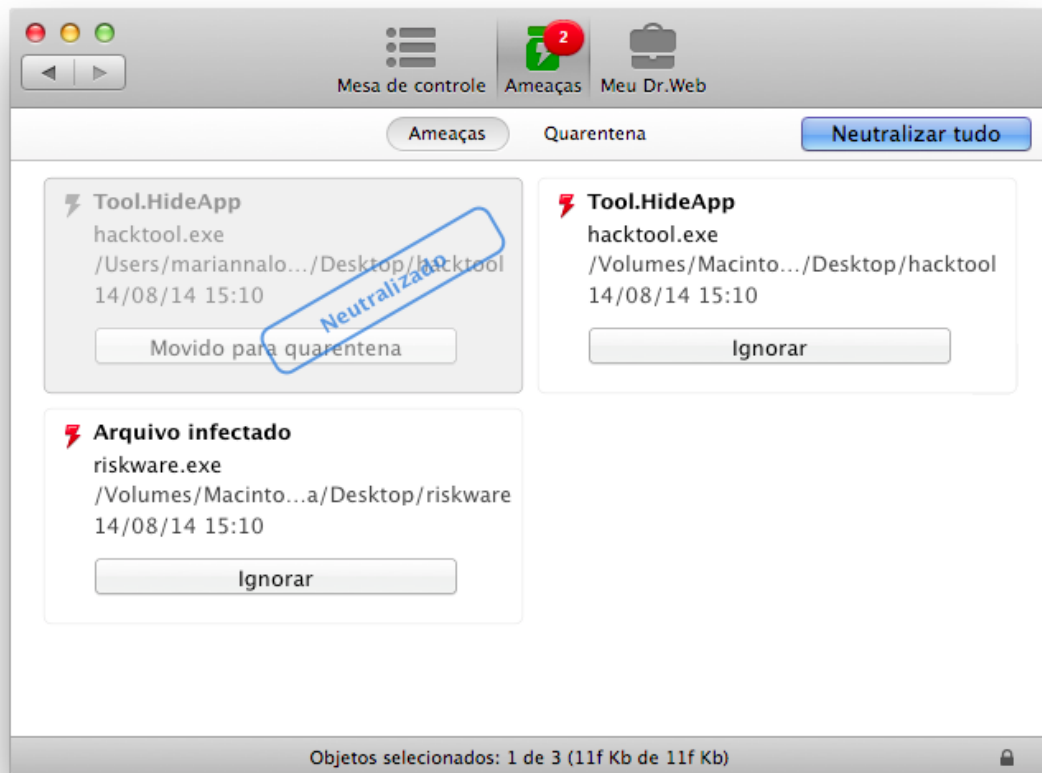
Imagem 3. Guia Ameaças.

Para ver informações sobre as ameaças

1. Para ver a lista de ameaças detectadas, abra a seção **Ameaças**. A barra de status, na parte inferior da janela, exibe o número total de ameaças e o tamanho de cada uma delas.
2. Para ver informações sobre uma ameaça, clique no botão ou clique duas vezes na ameaça.
3. Para ler sobre o tipo de ameaça no site da **Doctor Web**, clique no botão , à esquerda do nome da ameaça, na janela de detalhes.

Para neutralizar as ameaças detectadas

1. Abra a seção **Ameaças**.
2. Para aplicar uma ação especificada nas configurações do antivírus para o tipo de ameaça correspondente, clique no botão com esta ação, na ameaça. Para selecionar uma ação alternativa, clique na seta no botão com a ação recomendada, na janela de detalhes.
3. Para neutralizar vários objetos, selecione-os (mantenha a tecla SHIFT pressionada para selecionar vários objetos) e selecione a ação a ser executada, na seção **Ações**, no menu principal do aplicativo ou no menu que se abre com um clique no botão direito do mouse na lista de ameaças.

4. Para neutralizar todas as ameaças, clique em **Neutralizar todas**. Com isso, serão aplicadas ações especificadas nas configurações do antivírus para os tipos de ameaças correspondentes.

Também é possível usar as combinações de teclas de atalho no teclado, para aplicar ações às ameaças.

Verificação do tráfego HTTP e controle do acesso a recursos da Web

A verificação do tráfego na Web é realizada por um componente residente chamado **SpIDer Gate**. Ele verifica o tráfego HTTP recebido e bloqueia todos os objetos que contêm ameaças à segurança. O HTTP é usado por navegadores da Web, gerenciadores de download e outros aplicativos que compartilham dados com servidores Web, ou seja, que funcionam com a Internet.

O **SpIDer Gate** também permite que você controle o acesso a recursos da Web e impede que os usuários abram sites indesejados (como páginas sobre violência, jogos de azar, conteúdo adulto etc.).

Por padrão, o **SpIDer Gate** é habilitado automaticamente, depois que você instala e registra o **Dr.Web Anti-virus**.

É possível que outros aplicativos de verificação do tráfego da Web e controle de acesso aos recursos da Web instalados no seu Mac não funcionem adequadamente, quando o **SpIDer Gate** estiver habilitado.

Para habilitar ou desabilitar o SpIDer Gate

- Na seção **Mesa de controle** da janela principal (veja a Imagem 1), habilite/desabilite a opção **SpIDer Gate**.
- Clique no ícone do **Dr.Web Anti-virus** na barra de menus e selecione o item correspondente.

Somente usuários com privilégios de administradores podem desabilitar o **SpIDer Gate**.

Para configurar a verificação do tráfego HTTP

Por padrão, o **SpIDer Gate** bloqueia todos os objetos mal-intencionados recebidos. Você pode selecionar os tipos de programas mal-intencionados que deseja bloquear, configurar ações para os objetos não verificados e configurar o tempo máximo de verificação de um arquivo, seguindo estas instruções:

1. No menu do aplicativo, clique em **Preferências** e abra a guia **SpIDer Gate**. Somente usuários com privilégios de administrador podem alterar as configurações do **SpIDer Gate**. Clique no ícone de cadeado, no canto inferior da janela, e insira a senha e o nome de administrador, se for necessário.
2. Clique em **Avançado**.
3. Selecione os tipos de malware que você deseja bloquear.
4. Especifique o tempo máximo de verificação de um arquivo. Em alguns casos, o aumento do tempo de verificação de um único arquivo pode reduzir o desempenho do seu Mac.
5. Por padrão, os objetos que não podem ser verificados são bloqueados. Para permitir esses objetos, desmarque a caixa de seleção **Bloquear conteúdo não verificado**.
6. Clique em **OK**, para salvar as alterações.

Para configurar o acesso a sites

Por padrão, além da verificação antivírus do tráfego HTTP, o **SpIDer Gate** bloqueia URLs listadas como sites não recomendados ou devido a uma notificação do proprietário dos direitos autorais. Você pode desabilitar essas funções na guia **SpIDer Gate**, nas preferências do **Dr.Web Anti-virus**. Também é possível selecionar categorias de sites aos quais você deseja bloquear o acesso e criar listas de permissões e bloqueios de sites, para permitir ou bloquear automaticamente o acesso a eles, independentemente das configurações do **SpIDer Gate**.

As configurações padrão do **SpIDer Gate** são ideais, na maioria dos casos. Não altere-as se não houver necessidade.

Para configurar os parâmetros de bloqueio de sites:

1. No menu do aplicativo, clique em **Preferências** e abra a guia **SpIDer Gate**. Somente usuários com privilégios de administrador podem alterar as configurações do **SpIDer Gate**. Clique no ícone de cadeado, no canto inferior da janela, e insira a senha e o nome de administrador, se for necessário.
2. Selecione as categorias de sites aos quais você deseja bloquear o acesso.
3. Para criar e gerenciar as listas de permissões e bloqueios de URLs, clique em **Listas de permissões e bloqueios**. Por padrão, ambas as listas estão em branco. Você pode adicionar endereços às listas de permissões e bloqueios. Clique [+] na lista correspondente e insira um nome de domínio ou parte do nome do domínio do site ao qual você deseja bloquear ou permitir o acesso:
   - Para adicionar um site, insira o nome dele (por exemplo, **www.exemplo.com**). Esta ação permite o acesso a todas as páginas localizadas no site.
   - Para permitir o acesso a sites com nomes semelhantes, insira a parte em comum dos nomes do domínio. Por exemplo, se você inserir exemplo, o **SpIDer Gate** permitirá o acesso a **exemplo.com**, **exemplo.teste.com**, **teste.com/exemplo**, **teste.exemplo222.com** e outros sites semelhantes.
   - Para permitir o acesso aos sites de um domínio específico, insira o nome do domínio com um ponto ("**.**"). Esta ação permite o acesso a todas as páginas localizadas no site. Se o nome do domínio incluir uma barra ("**/**"), a subcadeia antes da barra será considerada um nome de domínio, e a subcadeia depois da barra será considerada parte do endereço dos sites que você quer acessar neste domínio. Por exemplo, se você inserir **exemplo.com/teste**, o **SpIDer Gate** permitirá o acesso a páginas como **exemplo.com/teste11**, **modelo.exemplo.com/teste22** e assim por diante.

   Para excluir sites da lista de permissões ou bloqueios, selecione-os na lista correspondente e clique em [−] ou arraste-os para fora da janela do aplicativo.
4. Clique em **OK**, para salvar as alterações.

Obter ajuda

Para obter assistência com o programa, você pode usar a **Ajuda do Dr.Web**, que pode ser acessada pelo Help Viewer da Apple.

Para acessar a Ajuda do Dr.Web

Na barra de menu, clique em **Ajuda** e selecione **Ajuda do Dr.Web**, ou pesquise por palavras-chave, na caixa de texto.

Caso não consiga encontrar uma solução para o problema ou informações necessárias sobre o **Dr.Web Anti-virus**, você pode solicitar assistência direta do suporte técnico.

Capítulo 5. Uso avançado

Este capítulo contém informações sobre como executar tarefas avanças com o **Dr.Web Anti-virus** e como ajustar suas configurações.

Quarentena

A quarentena permite que você isole objetos mal-intencionados ou suspeitos que foram detectados e que não podem ser curados no sistema, caso você precise deles. Os algoritmos de cura estão em constante aprimoramento, por isso esses objetos podem se tornar curáveis após uma das atualizações.

Por motivos de privacidade, é criada uma pasta de quarentena para cada usuário no sistema. Por esse motivo, as ameaças detectadas que foram movidas para a **Quarentena** do administrador durante o modo de administrador não estarão disponíveis nas pastas de **Quarentena** dos usuários.

Para ver e gerenciar o conteúdo da quarentena, use a guia **Quarentena**, na seção **Ameaças** da janela principal (veja a ilustração abaixo). A barra de status, na parte inferior da janela, exibe o número total de ameaças e o tamanho de cada uma delas.
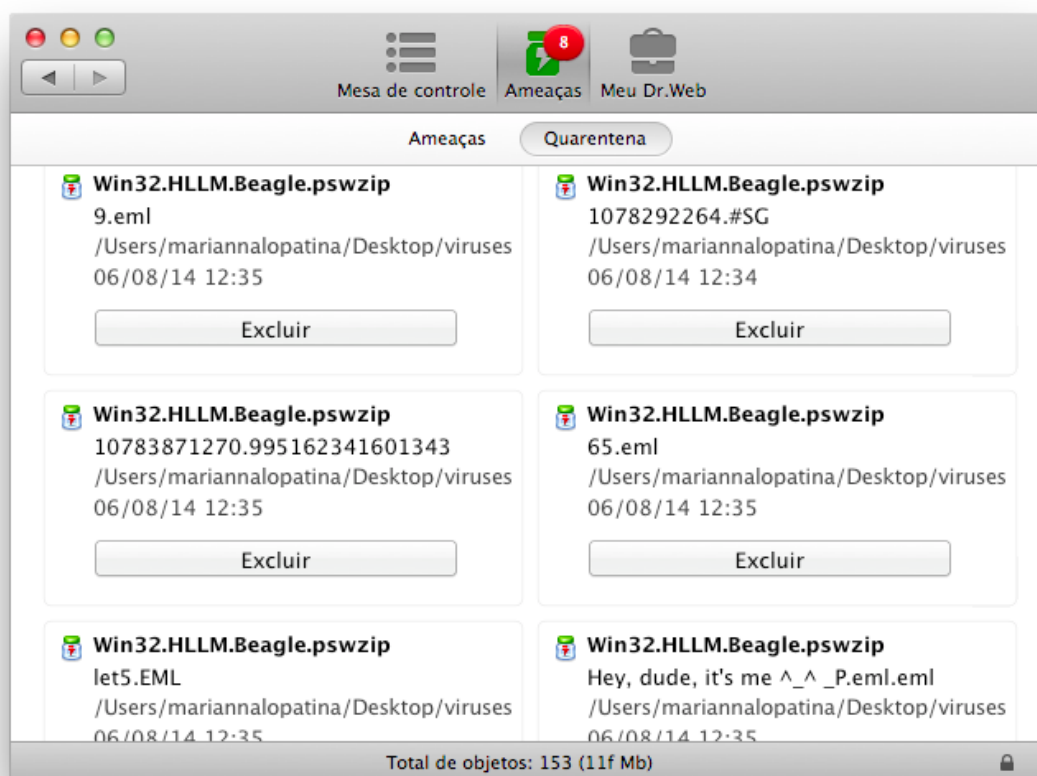
Imagem 4. Objetos em quarentena.

Para ver informações sobre os objetos em quarentena

1. Clique no botão ou clique duas vezes no objeto.
2. Para ler sobre o tipo de ameaça que o objeto aparenta conter no site da **Doctor Web**, clique no botão , à esquerda do nome da ameaça, na janela de detalhes. Será aberta uma página com informações sobre esse tipo de ameaça, no site da **Doctor Web**.

Para processar objetos na Quarentena

1. Para aplicar uma ação recomendada a um objeto em quarentena, clique no botão correspondente à ação, no objeto. Para selecionar uma ação alternativa, clique na seta no botão com a ação recomendada, na janela de detalhes. Você pode selecionar uma das seguintes ações:
   - **Excluir** – para remover completamente o objeto do sistema de arquivos.
   - **Curar** – para realizar outra tentativa de curar o objeto.
   - **Restaurar** – para tirar o objeto da quarentena e retorná-lo à pasta inicial de onde ele saiu.
   - **Restaurar para** – para selecionar a pasta para mover o objeto da quarentena.
2. Para processar vários objetos, selecione-os (mantenha a tecla SHIFT pressionada para selecionar vários objetos) e selecione a ação a ser executada, na seção **Ações**, no menu principal do aplicativo ou no menu que se abre com um clique no botão direito do mouse na lista de ameaças.

Também é possível usar as combinações de teclas de atalho no teclado, para aplicar ações aos objetos em quarentena.

Configuração de ações automáticas

Você pode especificar as ações que serão aplicadas automaticamente pelo **Dr.Web Anti-virus** para vários tipos de ameaças no computador, a menos que prefira escolher uma ação manualmente. Você pode definir diferentes reações do Verificador e para o **Verificador** e do **SpIDer Guard**.

Para configurar ações automáticas

1. Para abrir as configurações de reações automáticas dos componentes do **Dr.Web Anti-virus**, siga uma destas instruções:
   - Para configurações ações automáticas do **Verificador**, no menu do aplicativo, clique em **Preferências** e abra a guia **Verificador**.
   - Para configurações ações automáticas do **SpIDer Guard**, no menu do aplicativo, clique em **Preferências** e abra a guia **SpIDer Guard**.
2. Selecione a ação necessária para objetos infectados, incuráveis e suspeitos.
3. Clique em **Outros** para selecionar ações para malware (adware, discadores, piadas, riskware e hacktools).
4. As ações especificadas nas configurações do **SpIDer Guard** serão aplicadas cada vez que uma ameaça for detectada por estes componentes. Para aplicar ações automaticamente às ameaças detectadas na verificação do sistema executada pelo **Verificador**, marque a caixa de seleção **Aplicar ações automaticamente**, na seção de configurações do **Verificador**.
5. Clique em **Avançado** para configurar a verificação de objetos complexos (arquivos compactados e arquivos de email) e especificar o tempo máximo de verificação de um único arquivo. A verificação do conteúdo de arquivos compactados e arquivos de email, assim como o aumento do tempo de verificação de um único arquivo, aumenta o tempo total de verificação e, em alguns casos, pode reduzir o desempenho do seu Mac.

As ações automáticas padrão são ideais, na maioria dos casos. Não altere-as se não houver necessidade.

Por padrão, todas as configurações do **SpIDer Guard** são bloqueadas, para impedir que um usuário sem privilégios de administrador as altere. Para desbloqueá-las, selecione a seção **SpIDer Guard** das preferências do antivírus, clique no ícone de cadeado, na parte inferior da janela, e insira a senha e o nome de administrador.

Excluir arquivos da verificação

Você pode criar uma lista de arquivos e pastas que devem ser excluídos da verificação. Você pode definir diferentes exclusões para o **Verificador** e para o **SpIDer Guard**.

Para configurar exclusões

1. No menu do aplicativo, clique em **Preferências** e abra a guia **Exclusões**.
2. Marque as caixas de seleção ao lado dos objetos na lista de exclusões do **SpIDer Guard** e/ou do **Verificador**, para excluí-los da verificação.
3. Modifique a lista de exclusões, se for necessário:
   - Para adicionar um arquivo ou uma pasta à lista, clique no botão + e selecione o objeto.
   - Para excluir um objeto da lista de exclusões, selecione-o e clique em − ou arraste-o para fora da janela do aplicativo.

Por padrão, todas as pastas da quarentena são excluídas da verificação de ambos os componentes, porque são usadas para isolar ameaças detectadas e, como o acesso a elas é bloqueado, não há por que verificá-las.

As configurações padrão de exclusões são ideais, na maioria dos casos. Não altere-as se não houver necessidade.

Por padrão, todas as configurações do **SpIDer Guard** são bloqueadas, para impedir que um usuário sem privilégios de administrador as altere. Para desbloqueá-las, clique no ícone de cadeado, no canto inferior da janela, e insira a senha e o nome de administrador.

Notificações

As notificações sobre diversos eventos que podem ocorrer durante o funcionamento do antivírus são configuradas na guia **Principal**, nas preferências do **Dr.Web Anti-virus**.

Há 2 tipos de notificações:

- Mensagens visuais
- Alertas sonoros

Por padrão, as configurações de notificações são bloqueadas, para impedir que um usuário sem privilégios de administrador as altere. Para desbloqueá-las, clique no ícone de cadeado, na parte inferior da janela de preferências, e insira a senha e o nome de administrador.

Para configurar notificações sonoras

Os alertas sonoros são habilitados por padrão. Para desabilitar ou habilitar os alertas sonoros, marque ou desmarque a caixa de seleção **Usar alertas de som** da guia **Principal**, nas preferências do aplicativo.

Para configurar notificações visuais

1. As notificações visuais são habilitadas por padrão. Para desabilitar ou habilitar os alertas visuais, marque ou desmarque a caixa de seleção **Habilitar notificações** da guia **Principal**, nas preferências do aplicativo.
2. Selecione o sistema de notificações:
   - **Dr.Web** (selecionado por padrão)
   - **Sistema** (notificações padrão do Mac OS X)
   - **Growl**
3. Para as notificações do **Dr.Web**, você pode configurar parâmetros adicionais, clicando em **Configurar**, à direita do sistema de notificações selecionado:
   - Especificar o tempo de exibição das notificações
   - Selecionar a área na tela para mostrar as notificações

   Clique em **OK** para aplicar as configurações.

Privilégios de Administrador

O **Dr.Web Anti-virus** pode exigir privilégios de administrador para acessar e verificar áreas críticas do disco rígido. Para iniciar a verificação com privilégios de administrador:

1. No menu do aplicativo, clique em **Preferências** e abra a guia **Principal**.
2. Marque a caixa de seleção **Iniciar a verificação com privilégios de administrador**. Você precisará inserir a senha de administrador antes de iniciar a verificação (expressa, completa ou personalizada).

Otimizar o uso da bateria

Por padrão, se o Mac estiver usando a energia da bateria, a verificação é pausada, para evitar que a bateria se esgote rapidamente. O **Dr.Web Anti-virus** exibe uma mensagem correspondente, para você confirmar se deseja continuar a verificação. Para desabilitar a pausa da verificação:

1. No menu do aplicativo, clique em **Preferências** e abra a guia **Principal**.
2. Se você não quiser pausar a verificação quando o Mac estiver usando a energia da bateria, desmarque a caixa de seleção **Pausar a verificação no modo de bateria**.

Modo de operação

Se necessário, você pode usar sua instalação do **Dr.Web Anti-virus** para se conectar a redes corporativas de antivírus ou para acessar o serviço de antivírus **Dr.Web® AV-Desk** do seu provedor de TI. Para utilizar esse modo de proteção central, você não precisa instalar softwares adicionais nem desinstalar o **Dr.Web Anti-virus**.

Por padrão, as configurações de modo do **Dr.Web Anti-virus** são bloqueadas, para impedir que um usuário sem privilégios administrativos as altere. Para desbloqueá-las, clique no ícone de cadeado, no canto inferior da janela de preferências do modo, e insira a senha e o nome de administrador.

Para usar o modo de proteção central

1. Entre em contato com um administrador de rede de antivírus da sua empresa ou um provedor de TI, para obter um arquivo de chave pública e parâmetros de conexão com o servidor de proteção central.
2. No menu do aplicativo, clique em **Preferências** e selecione **Modo**.
3. Para se conectar ao servidor de proteção central da sua empresa ou do seu provedor de TI,, marque a caixa de seleção **Habilitar modo de proteção central**.

   No modo de proteção central, a opção para iniciar e configurar atualizações manualmente está bloqueada. Alguns recursos e configurações do **Dr.Web Anti-virus**, particularmente relacionados à proteção constante e à verificação sob demanda, podem ser modificados e bloqueados em conformidade com a política de segurança da empresa ou de acordo com a lista de serviços adquiridos. O arquivo de chave para operar neste modo é recebido do servidor de proteção central. Seu arquivo de chave pessoal não é utilizado.

   No modo de proteção central, a verificação do computador pode ser executada manualmente ou de acordo com uma programação, diretamente do servidor.

4. Ao entrar no modo de proteção central, o **Dr.Web Anti-virus** restaura os parâmetros da conexão anterior. Se você estiver se conectando ao servidor pela primeira vez, ou os parâmetros da conexão foram alterados, faça o seguinte:

   O arquivo install.cfg fornecido pelo administrador da rede de antivírus contém configurações para conectar ao servidor de proteção central. Para usar este arquivo:

   1. Clique em **Outros** tipos de ativação, no **Gerenciador de Licenças**.
   2. Arraste o arquivo de configuração até a janela aberta ou clique na área pontilhada, para selecionar o arquivo.

   Se o arquivo estiver instalado, os campos para inserir as configurações de conexão serão especificados automaticamente.

   - Insira o endereço IP do servidor de proteção central fornecido pelo administrador da rede de antivírus.
   - Insira o número da porta usada para conectar ao servidor.
   - Arraste o arquivo de chave pública até a janela de configurações ou clique duas vezes na área da chave pública e navegue para selecionar o arquivo.
   - Opcionalmente, insira os parâmetros de autenticação: ID da estação (atribuída ao seu computador para registrá-lo no servidor) e a senha. Os valores inseridos são salvos no sistema Keychain. Dessa forma, você não precisará inseri-los novamente, quando se reconectar ao servidor.

Dependendo das configurações de autorização do servidor de proteção central, a estação pode ser conectada ao servidor por um dos seguintes modos:

- Como novo usuário. Neste caso, a aprovação no servidor pode ser necessária (a ID e a senha serão atribuídas automaticamente), ou a estação pode ser autorizada automaticamente, se o modo de autorização correspondente estiver especificado no servidor.
- Se a estação já tiver sido criada no servidor e tiver ID e senha, será autorizada automaticamente ao se conectar ao servidor, independentemente das configurações.

Para obter informações detalhadas sobre como conectar uma estação ao servidor, consulte os guias de administrador do **Centro de Controle Dr.Web** e do **Dr.Web AV-Desk**.

Para usar o modo autônomo

1. No menu do aplicativo, clique em **Preferências** e selecione **Modo**.
2. Para entrar no modo autônomo, desmarque a caixa de seleção **Habilitar modo de proteção central**.

   Quando você entra neste modo, todas as configurações do antivírus são desbloqueadas e restauradas de volta aos valores padrão. Você volta a ter acesso a todos os recursos de antivírus.
3. Para funcionar corretamente no modo autônomo, o **Dr.Web Anti-virus** requer um arquivo de chave pessoal válido. Os arquivos de chave recebidos do servidor de proteção central não podem ser usados neste modo. Se necessário, você pode receber ou atualizar um arquivo de chave pessoal com o Gerenciador de Licenças.

Restaurar configurações padrão

Se você encontrar dificuldades para configurar o **Dr.Web Anti-virus**, poderá restaurar as configurações padrão do aplicativo.

Por padrão, a opção de restaurar as configurações padrão é bloqueada, para impedir que um usuário sem privilégios de administrador a altere. Para desbloqueá-la, clique no ícone de cadeado, no canto inferior da janela, e insira a senha de administrador.

1. No menu do aplicativo, clique em **Preferências** e abra a guia **Principal**.
2. Clique em **Restaurar padrões**. Confirme a restauração das configurações padrão do aplicativo, clicando em **Restaurar agora**, na caixa de diálogo correspondente.

Apêndices

Apêndice A. Tipos de ameaças

Neste documento, o termo *"ameaça"* é definido como qualquer tipo de software potencialmente ou diretamente capaz de causar dano a um computador ou rede, comprometendo as informações ou os direitos do usuário (ou seja, um software mal-intencionado ou indesejado). Em um sentido mais amplo, o termo "ameaça" pode ser usado para indicar qualquer tipo de perigo em potencial à segurança do computador ou da rede (ou seja, vulnerabilidades que podem resultar em ataques de hackers).

Todos os tipos de programas listados abaixo têm a capacidade de prejudicar os dados ou a confidencialidade do usuário. Os programas que não ocultam sua presença (por exemplo, softwares de distribuição de lixo eletrônico e diversos analistas de tráfego) normalmente não são considerados ameaças, ainda que possam se tornar perigosos sob determinadas circunstâncias.

Segundo a classificação da **Doctor Web**, as ameaças se dividem em dois tipos, de acordo com o nível de gravidade:

- **Ameaças graves** – são ameaças clássicas, que podem executar ações destrutivas e ilegais no sistema automaticamente (apagar ou roubar dados importantes, causar pane em redes etc.). Este tipo de ameaça consiste em softwares que são tradicionalmente chamados de malware (software mal-intencionado), ou seja, vírus, worms e Trojans.
- **Ameaças secundárias** – são menos perigosas que as graves, mas podem ser usadas por terceiros, para a execução de atividades mal-intencionadas. Além disso, a simples presença de ameaças secundárias no sistema indica seu baixo nível de proteção. Entre os especialistas em segurança de TI, esse tipo de ameaça também é chamado de grayware ou PUP (a sigla em inglês para "programa potencialmente indesejado") e consiste nos seguintes tipos de programas: adware, discadores, piadas, riskware e hacktools.

Ameaças graves

Vírus de computador

Este tipo de ameaça se caracteriza pela capacidade de implementar seu código em outros objetos. Essa implementação é chamada de *infecção*. Na maioria dos casos, o arquivo infectado se torna um portador do vírus, e o código implementado não corresponde necessariamente ao original. A maioria dos vírus tem como objetivo danificar ou destruir dados do sistema.

Segundo a classificação da **Doctor Web**, os vírus se dividem de acordo com o tipo de objetos que infectam:

- **Vírus de arquivos** infectam arquivos do sistema operacional (geralmente arquivos executáveis e bibliotecas dinâmicas) e são ativados quando o arquivo infectado é executado.
- **Vírus de macro** são vírus que infectam documentos usados pelo Microsoft® Office e alguns outros aplicativos compatíveis com comandos de macro (geralmente escritos em Visual Basic). Comandos de macro são programas (macros) implementados, escritos em uma linguagem de programação totalmente funcional. Por exemplo, os macros do Microsoft® Word podem ser inicializados automaticamente quando um documento é aberto (fechado, salvo etc.).
- **Vírus de script** são criados com o uso de linguagens de script e normalmente infectam outros scripts (ex: arquivos de serviço de um sistema operacional). Eles também pode infectar outros formatos de arquivos que permitem a execução de script, tirando proveito de vulnerabilidades dos scripts de aplicativos Web.

* **Vírus de boot** infectam registros de inicialização de disquetes e partições ou registros de inicialização mestre de discos fixos. Requerem bem pouca memória e se mantêm prontos para continuar executando suas tarefas até que ocorra um roll-out, uma reinicialização ou o desligamento do sistema.

A maioria dos vírus têm algum tipo de proteção contra detecção. Os métodos de proteção são constantemente aprimorados, e há sempre novas formas de combatê-los sendo desenvolvidas. Todos os vírus também pode ser classificados de acordo com o tipo de proteção que usam:

* **Vírus criptografados** criptografam seu código a cada infecção para impedir que sejam detectados em um arquivo, setor de inicialização ou memória. Todas as cópias desses vírus contêm um pequeno fragmento de código comum (o procedimento de descriptografia), que pode ser usado como uma assinatura do vírus.
* **Vírus polimórficos** também criptografam seu código, mas além disso também geram um procedimento especial de descriptografia que é diferente em cada cópia do vírus. Isso significa que esses vírus não têm assinaturas de bytes.
* **Vírus furtivos** podem executar certas ações que disfarçam sua atividade e ocultam sua presença em um objeto infectado. Esses vírus obtêm as características de um objeto antes de infectá-lo e, em seguida, plantam essas características "falsas" que enganam o verificador que busca arquivos modificados.

Os vírus também podem ser classificados de acordo com a linguagem de programação em que foram escritos (na maioria dos casos, Assembler, linguagens de programação de alto nível, linguagens de script etc.) ou de acordo com os sistemas operacionais afetados.

Worms

Atualmente, os worms se encontram mais alastrados do que os vírus e outros tipos de ameaças. Assim como os vírus, são capazes de se reproduzir e disseminar suas cópias, mas não infectam outros programas e arquivos (ou seja, não precisam de arquivos hospedeiros para se espalharem). O worm se infiltra em um computador de uma rede global ou local (normalmente por meio de um anexo de email) e distribui suas cópias funcionais a outros computadores na rede. Ele pode começar a se distribuir a partir da ação de um usuário ou de forma automática, escolhendo os computadores que irá atacar.

Os worms não consistem necessariamente em um único arquivo (o "corpo"). Muitos deles têm uma parte infecciosa ("shellcode"), que é carregada na memória principal (RAM) e faz o download do corpo do worm por meio de um arquivo executável pela rede. Se apenas o shellcode estiver presente no sistema, o worm poderá ser excluído por meio de uma simples reinicialização do sistema (na qual a memória RAM é apagada e reiniciada). No entanto, se o corpo do worm se infiltrar no computador, somente um programa de antivírus poderá se livrar ele.

Os worms têm a capacidade de danificar redes inteiras, mesmo sem ter nenhuma carga destrutiva (ou seja, não causam nenhum dano direto), devido à sua intensa distribuição.

Segundo a classificação da **Doctor Web**, os worms estão divididos de acordo com o método de distribuição:

* **Worms de rede** distribuem suas cópias por meio de diversos protocolos de rede e de compartilhamento de arquivos.
* **Worms de email** se espalham com o uso de protocolos de email (POP3, SMTP etc.).
* **Worms de chat** usam protocolos de programas populares de chat e mensagens (ICQ, IM, IRC etc.).

Programas de Trojan (Trojans)

Este tipo de ameaça não é capaz de se reproduzir nem de infectar outros programas. O Trojan substitui um programa que é muito usado e executa suas funções (ou imita seu funcionamento). E, ao mesmo tempo, executa ações mal-intencionadas no sistema (danifica ou exclui dados, envia informações confidenciais etc.) ou possibilita que um hacker acesse o computador sem permissão, por exemplo, para danificar o computador de terceiros.

Os recursos mal-intencionados e de mascaramento do Trojan são semelhantes aos de um vírus. Um Trojan pode até ser um componente de um vírus. No entanto, a maioria dos Trojans são distribuídos como arquivos executáveis individuais (por meio de servidores de transferência de arquivos, portadores de dados removíveis ou anexos de email) que são executados por usuários ou tarefas do sistema.

É muito difícil classificar os Trojans, porque costumam ser distribuídos por vírus ou worms, e também porque muitas ações mal-intencionadas que podem ser executadas por outros tipos de ameaças são atribuídas somente aos Trojans. Estes são alguns tipos de Trojan que são classificados separadamente pela **Doctor Web**:

- **Backdoors** são Trojans que permitem que invasores entrem no sistema e obtenham funções privilegiadas, contornando quaisquer medidas de acesso e segurança existentes. Os backdoors não infectam arquivos, mas se gravam no registro, modificando as chaves de registro.
- **Rootkits** são usados para interceptar funções de um sistema operacional para permanecerem ocultos. Além disso, um rootkit pode ocultar processos de outros programas (por exemplo, outras ameaças), chaves de registro, pastas e arquivos. Ele pode ser distribuído como um programa independente ou como componente de outro programa mal-intencionado. Há dois tipos de rootkits, de acordo com seu modo de operação: User Mode Rootkits (UMR), que funcionam no modo de usuário (interceptam funções de bibliotecas do modo de usuário) e Kernel Mode Rootkits (KMR), que operam no modo kernel (interceptam funções no nível do kernel do sistema, o que dificulta sua detecção).
- **Keyloggers** são usados para gravar dados que os usuários inserem por meio do teclado. O objetivo desse recurso é roubar informações pessoais (ex: senhas de rede, dados de logon, informações do cartão de crédito etc.).
- **Clickers** redirecionam hiperlinks para determinados endereços, para aumentar o tráfego de sites ou executar ataques de negação de serviço.
- **Trojans de proxy** fornecem acesso anônimo à Internet pelo computador de uma vítima.

Os Trojans também podem executar outras ações mal-intencionadas além das supracitadas, como, por exemplo, alterar a página inicial de um navegador da Web ou excluir determinados arquivos. No entanto, outras ações também podem ser realizadas por outros tipos de ameaças (vírus e worms).

Ameaças secundárias

Hacktools

Hacktools são programas desenvolvidos para ajudar o hacker em atividades ilegais. Os mais comuns entre eles são os verificadores de portas, que detectam vulnerabilidades em firewalls e em outros componentes do sistema de proteção do computador. Além de hackers, essas ferramentas também são usadas por administradores, para verificar a segurança de suas redes. Ocasionalmente softwares comuns que podem ser usados para hackear e diversos programas que usam técnicas de engenharia social também são classificados de hacktools.

Adware

Normalmente, este termo se refere a um código de programa implementado em programas freeware que força a exibição de anúncios para os usuários. No entanto, às vezes esses códigos podem ser distribuídos por meio de outros programas mal-intencionados e mostrar anúncios em navegadores da Web. Muitos programas de adware operam com dados coletados por spyware.

Piadas

Assim como o adware, este tipo de ameaça secundária não pode ser usado para causar danos diretos ao sistema. Os programas de piadas normalmente só geram mensagens sobre erros que nunca ocorreram e ameaçam executar ações que causarão perda de dados. O propósito desses programas é assustar ou irritar os usuários.

Discadores

São programas especiais desenvolvidos para buscar em um intervalo de números telefônicos aqueles que possuem a resposta de um modem. Esses números são, então, usados para elevar o preço de instalações telefônicas ou para conectar o usuário a serviços telefônicos caros.

Riskware

Estes programas não são desenvolvidos originalmente como ameaças, mas podem danificar ou ser usados para danificar a segurança do sistema devido a alguns recursos. Por esse motivo, são classificados como ameaças secundárias. Os programas de riskware não são apenas aqueles que podem danificar ou excluir dados acidentalmente, mas também os que podem ser usados por invasores ou programas mal-intencionados para danificar o sistema. Entre eles estão diversos programas de chat e ferramentas administrativas remotas, servidores FTP etc.

Objetos suspeitos

São possíveis ameaças no computador detectadas pelo analisador heurístico. Esses objetos podem ser potencialmente qualquer tipo de ameaça (até desconhecidas para especialistas em segurança de TI) ou também podem ser perfeitamente seguros, no caso de uma falsa detecção.

Objetos suspeitos devem ser enviados ao **Laboratório de Vírus Dr.Web**, para análise.

Apêndice B. Como combater ameaças

As soluções de antivírus **Dr.Web** usam vários métodos simultâneos de detecção de softwares mal-intencionados, que permitem a elas executar verificações completas em arquivos suspeitos e controlar o comportamento do software.

Métodos de detecção

Análise de assinaturas

As verificações começam com a análise da assinatura, que é feita por meio da comparação de segmentos de código dos arquivos com assinaturas de vírus conhecidos. A *assinatura* sequência contínua e finita de bytes que é necessária e suficiente para identificar um vírus específico. Para reduzir o tamanho do dicionário de assinaturas, as soluções de antivírus **Dr.Web** usam somas de verificação de assinaturas, em vez de sequências de assinaturas completas. As somas de verificação identificam as assinaturas de modo único, mantendo a exatidão da detecção e da neutralização dos vírus. Os **bancos de dados de vírus Dr.Web** são compostos, para que algumas entradas possam ser usadas para detectar não apenas vírus específicos, mas classes inteiras de ameaças.

Origins Tracing

Ao concluir a análise de assinaturas, as soluções de antivírus **Dr.Web** usam o método exclusivo **Origins Tracing™** para detectar vírus novos e modificados, que usam mecanismos conhecidos de infecção. Por isso, os usuários do **Dr.Web** estão protegidos contra ameaças como o famigerado Trojan.Encoder.18 (também conhecido como gpcode). Além da detecção de vírus novos e modificados, o mecanismo **Origins Tracing™** proporciona uma redução drástica no número de alarmes falsos do analisador heurístico. Os objetos detectados com o uso do algoritmo **Origins Tracing™** são indicados com a extensão `.Origin` adicionada aos seus nomes.

Emulação de execução

A tecnologia de emulação de códigos de programa é usada para detectar vírus polimórficos e criptografados, quando a busca com somas de verificação não pode ser aplicada diretamente ou é muito difícil de ser executada (devido à impossibilidade de criar assinaturas seguras). O método simula a execução de um código analisado por um *emulador* (um modelo de programação do ambiente de tempo de execução e do processador). O emulador opera com a área de memória protegida (*buffer de emulação*), no qual a execução do programa analisado é modelada, instrução por instrução. No entanto, nenhuma dessas instruções é executada realmente pela CPU. Quando o emulador recebe um arquivo infectado com um vírus polimórfico, o resultado da emulação é um corpo de vírus criptografado que, em seguida, é facilmente determinado com a busca por soma de verificação de assinatura.

Análise heurística

O método de detecção usado pelo analisador heurístico é baseado em determinados conhecimentos (*heurística*) sobre certos recursos (atributos) que podem ser típicos do próprio código de vírus e vice-versa, que são extremamente raros em vírus. Cada atributo tem um coeficiente de peso que determina seu nível de gravidade e confiabilidade. O coeficiente de peso pode ser positivo, se o atributo correspondente for indicativo de um código mal-intencionado, ou negativo, se o atributo for atípico de uma ameaça. Dependendo do peso da soma de um arquivo, o analisador heurístico calcula a probabilidade de infecção pelo vírus desconhecido. Se o limite for ultrapassado, o analisador heurístico concluirá que o objeto analisado provavelmente está infectado por um vírus desconhecido.

O analisador heurístico também usa a tecnologia **FLY-CODE™**, que é um algoritmo versátil para a extração de arquivos. A tecnologia permite fazer suposições heurísticas sobre a presença de objetos mal-intencionados em arquivos compactados não apenas por empacotadores que o **Dr.Web** reconhece, mas também por programas novos e até então inexplorados. Ao verificar objetos empacotados, as soluções de antivírus **Dr.Web** também usam análises de entropia estrutural. A tecnologia detecta ameaças organizando partes do código. Assim, uma entrada do banco de dados permite a identificação

de uma porção substancial de ameaças empacotadas com o mesmo empacotador polimórfico.

Como qualquer sistema de teste de hipóteses em caso de incerteza, o analisador heurístico pode cometer erros do tipo I ou II (omitir vírus ou emitir alarmes falsos). Sendo assim, os objetos detectados pelo analisador heurístico são tratados como "suspeitos".

Ao executar qualquer uma das verificações supracitadas, as soluções de antivírus **Dr.Web** usam as informações mais recentes sobre softwares mal-intencionados conhecidos. Assim que os especialistas do **Laboratório de Vírus Doctor Web** descobrem novas ameaças, são lançadas atualizações com assinaturas de vírus, atributos e características de comportamentos. Em alguns casos, em apenas uma hora podem ser lançadas várias atualizações. Por isso, mesmo se um vírus inédito passar pela proteção residente **Dr.Web** e penetrar o sistema, depois de uma atualização, ele será detectado na lista de processos e neutralizado.

Ações

Para neutralizar as ameaças no computador, os **produtos Dr.Web** usam inúmeras ações que podem ser aplicadas a objetos mal-intencionados. O usuário pode manter as configurações padrão, configurar as ações a serem aplicadas automaticamente ou escolher as ações manualmente a cada detecção. Apresentamos abaixo uma lista das possíveis ações:

- **Cura** é uma ação que só pode ser aplicada às ameaças graves (vírus, worms e Trojans). Ela implica na exclusão do código mal-intencionado de objetos infectados, assim como a recuperação da estrutura e da operabilidade, de volta ao estado anterior à infecção, se possível. Às vezes, os objetos mal-intencionados são formados apenas de código mal-intencionado (por exemplo, Trojans ou cópias funcionais de worms) e, para que sejam curados, o sistema precisa removê-los por completo. Nem todos os arquivos infectados por vírus podem ser curados, mas os algoritmos de cura estão sempre evoluindo.
- **Quarentena** (Mover para Quarentena) é uma ação realizada quando a ameaça detectada é enviada para uma pasta especial e isolada do resto do sistema. Essa ação é preferível quando a cura é impossível e para todos os objetos suspeitos. Recomendamos que o usuário envie cópias desses arquivos para o **Laboratório de Vírus Dr.Web**, para análise.
- **Excluir** é a ação mais eficaz para neutralizar ameaças no computador. Pode ser aplicada a qualquer tipo de ameaça. A exclusão será às vezes aplicada a alguns objetos para os quais a ação Sanar foi selecionada. Isso acontece quando o objeto é formado apenas pelo código mal-intencionado e não tem informações úteis (por exemplo, a cura de um worm implica na exclusão de todas as suas cópias funcionais).
- **Renomear** é uma ação realizada quando a extensão de um arquivo infectado é alterada de acordo com uma máscara especificada (por padrão, o primeiro caractere da extensão é substituído por #). Esta ação pode ser apropriada para arquivos de outros sistemas operacionais (como MS-DOS® ou Microsoft® Windows®) detectados como suspeitos pela análise heurística. A renomeação pode evitar a inicialização acidental de arquivos executáveis nesses sistemas operacionais, impedindo, assim, a infecção por um possível vírus e sua posterior expansão.
- **Ignorar** é uma ação aplicada apenas às ameaças secundárias (ou seja, adware, discadores, piadas, hacktools e riskware). Ela permite ignorar a ameaça, sem realizar nenhuma ação nem exibir relatórios.
- **Relatório** significa que nenhuma ação é aplicada ao objeto, e a ameaça é apenas listada no relatório de resultados.

Apêndice C. Proteção central de antivírus

As soluções de proteção central da **Doctor Web** ajudam a automatizar e simplificar a configuração e o gerenciamento da segurança de informações de computadores em estruturas lógicas (por exemplo, computadores de uma empresa que acessam um ao outro de dentro e fora das redes locais da empresa). Os computadores protegidos são reunidos em uma rede de antivírus cuja segurança é monitorada e gerenciada a partir do servidor central por administradores. A conexão aos sistemas centralizados de antivírus garante um alto nível de proteção e requer esforços mínimos para os usuários finais.

Estrutura lógica de redes de antivírus

As soluções de proteção central da **Doctor Web** usam o modelo servidor-cliente (veja a imagem abaixo).

As estações de trabalho e os servidores são protegidos por *componentes locais de antivírus* (agentes ou clientes; **Dr.Web Anti-virus**) instalados neles, que fornecem proteção de antivírus a partir de computadores remotos e garantem uma fácil conexão ao servidor de proteção central.
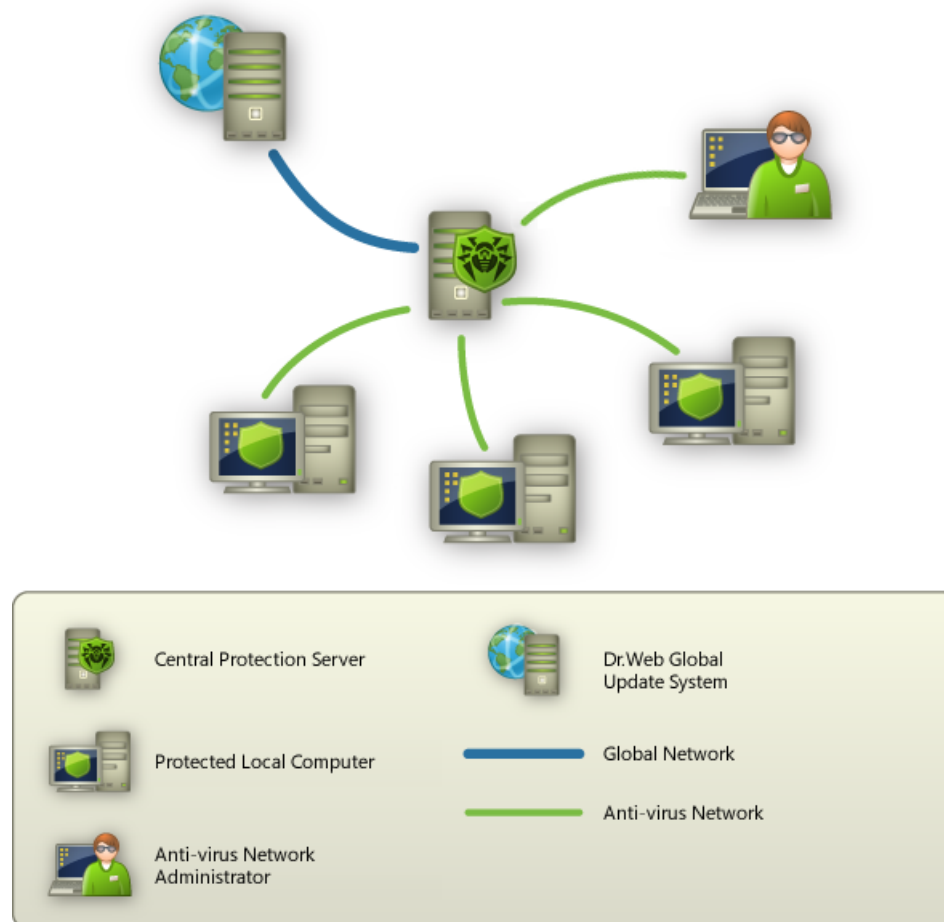
Imagem 5. Estrutura lógica de redes de antivírus

Os computadores locais são atualizados e configurados a partir do *servidor central*. O fluxo de instruções, dados e estatísticas na rede de antivírus também é originado do servidor de proteção central. O volume de tráfego entre os computadores protegidos e o servidor central poderá ser considerável, por isso as soluções oferecem opções de compactação do tráfego. Para impedir o vazamento de dados confidenciais ou a substituição de softwares baixados nos computadores

protegidos, também há suporte para criptografia.

Todas as atualizações necessárias são baixadas para o servidor de proteção central a partir dos servidores do **Sistema de Atualização Global da Dr.Web**.

Os componentes locais de antivírus são configurados e gerenciados pelo servidor de proteção central, de acordo com os comandos dos *administradores da rede de antivírus*. Os administradores gerenciam servidores de proteção central e a topologia de redes de antivírus (por exemplo, validando conexões ao servidor de proteção central a partir de computadores remotos), e configuram o funcionamento dos componentes locais de antivírus, quando necessário.

Os componentes locais de antivírus não são compatíveis com outros softwares de antivírus, incluindo versões de **soluções de antivírus Dr.Web** que não funcionam com o modo de proteção central (ex: **Antivírus Dr.Web para Mac OS X** versão 5.0). A instalação de dois programas de antivírus no mesmo computador pode causar falhas no sistema e perda de dados importantes.

Soluções de proteção central

Dr.Web® Enterprise Security Suite

Dr.Web® Enterprise Security Suite é uma solução complexa para redes corporativas de qualquer tamanho, que oferece proteção confiável contra todos os tipos de ameaças atuais, para estações de trabalho e servidores de arquivos e correio. Esta solução também oferece diversas ferramentas para administradores de redes de antivírus, que permitem o rastreamento e o gerenciamento da operação de componentes locais de antivírus, incluindo a implantação e atualização de componentes, o monitoramento do status da rede, a coleta de estatísticas e a notificação sobre eventos de vírus.

Serviço de Internet Dr.Web® AV-Desk

Dr.Web® AV-Desk é um inovador serviço de Internet, criado pela **Doctor Web**, para provedores de diversos tipos de serviços de Internet. Com esta solução, os provedores podem oferecer serviços de segurança de informações a clientes domésticos e empresariais, com um pacote selecionado de serviços de proteção contra vírus, lixo eletrônico e outros tipos de ameaças, pelo tempo que for necessário. Os serviços são fornecidos online.

Para obter mais informações sobre o serviços de Internet **Dr.Web® AV-Desk** visite o site oficial da **Doctor Web**, em http://www.av-desk.com.

Apêndice D. Teclas de atalho

Você pode usar as combinações especiais de teclas de atalho para iniciar uma verificação no sistema, para aplicar uma ação às ameaças detectadas ou para configurar o **Dr.Web Anti-virus**.

Combinação		Descrição
Menu de verificação	CONTROL-COMMAND-E	Verificação expressa
	CONTROL-COMMAND-F	Verificação completa
	CONTROL-COMMAND-C	Selecionar objetos para verificar
Menu de ações	COMMAND-SHIFT-C	Sanar
	COMMAND-SHIFT-M	Mover para quarentena
	COMMAND-SHIFT-I	Ignorar
	COMMAND-SHIFT-D	Excluir
	COMMAND-SHIFT-R	Restaurar
	COMMAND-SHIFT-P	Restaurar para
	COMMAND-SHIFT-A	Trabalhar com privilégios de administrador
Geral	COMMAND-,	Preferências
	COMMAND-A	Selecionar tudo
	COMMAND-W	Fechar

Apêndice E. Contato com o suporte

Em caso de problemas na instalação ou no uso de produtos da empresa, utilize as seguintes opções de suporte da **Doctor Web**:

- Baixe e consulte os manuais e guias mais recentes em http://download.drweb.com/
- Leia as perguntas frequentes em http://support.drweb.com/
- Visite o fórum oficial **Dr.Web** em http://forum.drweb.com/

Caso não encontre solução para o problema, solicite assistência direta do **suporte técnico Doctor Web**, preenchendo o formulário na seção correspondente do site de suporte, emhttp://support.drweb.com/.

Para obter informações sobre escritórios regionais, visite o **site oficial da Doctor Web**, em http://company.drweb.com/contacts/moscow.

Índice

Índice